OPERATIONS CHAPTER 13

(FILE NAME ON DISK # 1 = S2C13.WPD)

The computer operations department is responsible for selecting, operating and maintaining computer and telecommunications equipment that retain and process information assets of the institution. The department must maintain a stable production environment, process the data promptly and efficiently, and protect the data files, programs, and equipment under its control.

The computer operations department generally has responsibility for the following functions:

- Computer operations.
- Communications network control.
- Data preparation.
- Transaction processing.
- Workload scheduling.
- Media library.
- Documentation library.
- Performance monitoring.
- Disaster contingency planning.

The controls described in this section generally describe centralized computer facilities. However, the concepts also apply to end-user computing systems located throughout the organization.

In order to perform their job functions, computer operations personnel must have access to the information necessary to run various equipment and programs. All information for processing work should appear in the Operator's Run Manuals. The information should be limited to the functions to be performed, the hardware, software and data files to be used for processing, and maintenance of the equipment. Run manuals normally include processing procedures, rerun instructions, special application instructions, file rotation procedures, recovery instructions, and emergency procedures. Computer operators should not have access to software or hardware documentation that is not necessary to perform their duties. Management, assisted by computer operations and systems development and programming personnel, must ensure that Operator's Run manuals are current.

There also should be an overall procedures manual for all computer operations functions. This manual should cover matters, such as equipment maintenance, equipment operation, staff policies, and coordination with other departments.

Just as computer operators must have sufficient instructions to run the system, users must have the necessary information to properly use applications. User manuals providing information on the preparation and control of source documents, along with the control, use, and format of output should be readily available. The user manual should include examples of documents and sufficient details about the reconcilement of applications.

SEPARATION AND ROTATION OF DUTIES

Operations management must implement policies and procedures for separating and rotating duties, and cross-training personnel. The size of the installation will influence the types of policies implemented for the division of duties.

Separation of duties is a basic internal control procedure. Management must assign duties to separate responsibility for different elements of computer operations and application processing. Computer operators should not perform any duties other than those directly relating to equipment operation. However, this is not meant to prohibit operators from learning other duties or from performing them in an emergency. For example, there should be no overlap between computer operations and data preparation for processing. Generally, computer operators should not perform duties such as reject re-entry, general ledger balancing, or unposted items settlement. No one should be permitted to perform one function from start to finish or be responsible for checking the accuracy of his or her own work. In all areas of the financial institution, separation of duties is the best deterrent against employee dishonesty or intentional harm to equipment, documentation, or records. If this control is present, a person wishing to subvert the system is forced into collusion with other personnel.

Rotation of duties serves as both an internal control and cross-training tool. Tasks and shifts should be rotated among computer operators to: provide each operator with training for operational tasks, and prevent operators from handling any one function indefinitely. Rotation of employees should be of sufficient duration to permit disclosure of any irregularities. The implementation of rotation assignments, in large measure, depends on the size of the installation.

In smaller institutions, where there is little separation of duties, rotating duties takes on added significance as an internal control measure. The actual rotation should be logged to document performance. When people normally not responsible for running the computer act as operators, computer time must be closely controlled, and continual management review of the conflicting functions is necessary. As in other departments, mandatory vacations for at least two consecutive weeks should be encouraged for all IS personnel.

In large centers with separation of duties, the possibility of an individual jeopardizing the integrity of the institution's information systems is minimized and rotation of duties is less important as an internal control. However, in such instances, rotation provides effective cross-training and should be used whenever possible.

EQUIPMENT MAINTENANCE

Preventive maintenance on equipment should be performed at all installations. This includes minor maintenance, such as cleaning peripheral equipment by center employees, as well as more extensive maintenance provided by the manufacturer or vendor. Computer operators should not be permitted to repair equipment or perform other than the most routine maintenance.

Maintenance by computer operators should be performed according to manufacturers' recommendations. As a general rule, these duties include:

- Cleaning tape heads each shift.
- Cleaning printers daily.
- Checking and cleaning the MICR reader/sorter at the end of each shift.

- Periodically checking and cleaning the area under raised flooring.

Maintenance schedules may vary considerably depending on the size of the installation and the volume of work processed. All maintenance should be performed according to a predetermined schedule, not on a random basis, and recorded in logs or other records. Management review of these records could aid in monitoring employee and vendor performance.

Maintenance by the manufacturer or vendor usually will be performed under contract. If equipment is leased from the manufacturer, the maintenance agreement may be part of the lease. When equipment is owned or leased from a third party, a separate maintenance/service agreement between the IS department and the equipment manufacturer should be used.

The service and maintenance agreement should provide repair services, detail the preventive maintenance to be performed, and indicate a schedule for both. When a center uses hardware from more than one manufacturer, maintenance boundaries should be defined. Under such conditions, it may be desirable to enter into an arrangement whereby one vendor takes responsibility for seeing that overall repair maintenance is accomplished. Under this arrangement, whenever hardware problems are encountered, the data center would contact the designated vendor to determine the source of the problem and to assure that vendor makes the necessary repairs. In any event, data center management should ensure that maintenance contracts guarantee timely performance.

A certain amount of computer time should be scheduled for preventive maintenance. During this maintenance, the service representative (computer engineer or customer engineer) will service the equipment, e.g., change filters, fill oil reservoirs, and check all indicator lights, hardware circuits, and other mechanisms. When this occurs, the computer operators should dismount all program and data files and work packs, leaving only the minimum software required for the specific maintenance task on the system. If this is impractical, appropriate systems activity logs must be reviewed by operations management to check security regarding access to programs during maintenance. Also, at least one computer operator should be present at all times when the service representative is in the computer room.

Operators should maintain a written log of all hardware problems and downtime encountered between maintenance sessions. A periodic report on the nature and frequency of those problems is a necessary management tool, and may be valuable for vendor selection, equipment benchmarking, replacement decisions, or planning increased equipment capacity.

EQUIPMENT OPERATIONS

Operation of the computer and its peripheral devices is best accomplished by following manufacturers' procedures and operator instructions. Manuals for equipment operation should be current, describing the computer system actually in use, and be readily available to computer operators.

Operator's instructions should include:

- Identification of all input/output forms (including samples of special forms).
- Instructions for forms alignment.
- Explanation of the run purpose.
- Detailed instructions for the disposition of input and output.
- Identification of all programmed halts and operator responses.
- Prescribed start and restart instructions.
- Description of records used and hardware requirements.
- Run frequency and priority.
- Sequence in which programs are to be executed.
- Description of all special instructions or conditions.

An operating log or file should be maintained to record any significant events and actions taken by computer operators. This usually would be prepared by the lead operator of each shift and inspected daily by operations management to ensure that operators are following instructions. IS management should restrict the use of computer equipment and media, and the actions of operators and other personnel whose duties affect the operation. These restrictions should be in written operating procedures. The procedures should be current and sufficiently detailed to guide operation of the computer center.

SCHEDULING

Computer workload scheduling is critical to efficient IS operations. Many data centers use automated scheduling programs. Applications run on large or highly sophisticated computer systems usually cannot be scheduled effectively without reliance on automated programs. Regardless of the complexity of the scheduling procedure, certain questions must be considered in all installations:

- Does the schedule make efficient use of computer resources? All users want their jobs run early to ensure prompt delivery. However, an efficiently operated center does not schedule production runs and produce reports for all applications during the prime processing shift, leaving the computer system idle for the remainder of the day. Neither does it schedule jobs to run so early that the provider of the input cannot be ready, or so late that the output will be delivered later than needed.
- Does the scheduling procedure take into consideration the late arrival of input? The schedule should contain cutoff times after which the job must be run with only available input or deferred until a later time. No job should be delayed indefinitely, thus holding up all others set to run after it. In certain cases, running an application with incomplete data may be inefficient; in other cases, it may be appropriate to run the application with available data only.
- Are all jobs assigned an overall priority rating? Priority ratings should be assigned to all jobs run on a regular basis so that critical applications will

be run first, after recovery from an emergency. For example, if such a priority system is not used, and there is a hardware failure (which can hold up processing for several hours), critical applications such as deposit applications, may be in the queue awaiting execution when the financial institution opens on the following day.

Non-routine computer runs should be supported by a work request or other written authorization. This includes all unscheduled production jobs, assemblies, compiles, and tests. All scheduling should include due-in/due-out times and dates of input and output; records covering delays in receipt of input, data processing and delivery of output; and adherence to priorities. Schedules, whether manual or computer prepared, should be compared against actual run times.

System usage reports indicating scheduled and unscheduled production time, program test and assembly time, reruns and maintenance periodically should be prepared. They should be reviewed by installation management, and variations from scheduled activity should be investigated. Additionally, the backlog of jobs awaiting processing by each shift should be reviewed for reasonableness.

BACKUP

The creation and rotation of backup tapes is a vital function of the operations area. Adequate onsite and offsite backup of operating systems, application programs, master data files, and transaction files is essential as processing systems are susceptible to many types of disruptions. Disruptions can be caused by system crashes, equipment problems, program or data file corruption, physical, environmental, or other types of site related disasters as discussed in Chapter 10. The lack of timely and comprehensive backup procedures may lead to significant expenses in reconstructing programs or data files, and could lead to operational failure. Backup files should be rotated offsite as soon as practical after creation to reduce an institution’s risk exposure.

Program File Backup

Program files generally consist of the operating system and application programs. In less complex systems these files will be located in a few libraries/directories and can easily be backed up by copying entire libraries to tape. More complex systems maintain many of libraries/directories and may require automated library systems to manage the backup process. Operations management periodically should review programs and the contents of program libraries/directories to ensure backup procedures are adequate. In more complex organizations, this review likely will require user input into the function and importance of files in their libraries.

At a minimum, program file backup should include:

- The current operating system.
- The object code version of production application programs.
- Source code files for production programs. (If programs are supported in-house)
- System utilities which are utilized by operations. (Includes text editors, compilers, etc. if programs are supported in-house)
- Any other programs which are necessary to restore operations at the recovery site.
- Documentation for all of the above.

This list provides a bare minimum of the program files needed to operate the computer as a snapshot of its current configuration. Many institutions also routinely backup source code program files, files in programming development libraries, files in programming test libraries, and other files as deemed appropriate. Backup tapes of program files should be created after every system update.

Master File and Transaction File Backup

Master files and transaction files requiring daily duplication and rotation off premises will vary. In any case, master files and transaction files sufficient to recreate the current day's master files must be stored both on and off premises, as backup for each application processed. For applications that do not produce a daily master file, a cumulative transaction journal should be used and backed up in the same manner as master files.

In a distributed data processing environment (LANs), disk mirroring and/or disk duplexing provides real time backup of data to a secondary disk, so that it can be used should the primary disk become nonfunctional. With mirroring, data and operations can continue immediately without any disruption to the user. Regardless of whether the LAN has disk mirroring and/or duplexing, institutions that process data on a LAN should store regular periodic backups of the programs and data offsite, using a similar retention methodology as with mainframe data (indicated above).

Because computer systems differ, the vendor should be asked for the most suitable backup rotation plan. If the only backup copy of files are stored in the computer area, a fire, or other disaster could destroy all machine-readable records. In that case, the institution would either be unable to create a current master file or have to recreate a machine-readable file from all available source documents. The latter option is expensive and time consuming. To avoid this situation, the financial institution should store a current copy of the master file and subsequent transaction files at a remote location. The remote location can be a fireproof box at a local business, another financial institution, a branch office or, as a last resort, at an employee's home. Although the location should be relatively secure, having data stored offsite even in a nonfireproof location is more desirable than no off-site storage, because simultaneous destruction is less likely. The key is that it must not be a site that is subject to the same disaster.

Some institutions will store all backup files in the main vault. Although this reduces risk and may be appropriate for paper documents with high heat tolerance, it is not the most desirable since off-site storage is almost as easy to implement and provides significantly more protection. If the computer facility is completely destroyed, the financial institution should be able to resume normal processing as soon as alternate equipment is available provided backup files are stored off-site.

Procedures relating to file retention and offsite-storage should normally require:

- Maintaining off-premises backup files in machine-readable form.
- Reducing the lag, and the potential exposure, between the creation of current master file backups and the rotation of these files to off-premises storage.
- Rotating new backup files to off-premises storage before returning old backup files to the data center.
- Keeping off-premises storage sites environmentally controlled and physically secure.

Procedures relating to the use of backup for data files and program libraries, whether in-house or remote, normally include:

- Recopying backup files prior to use.
- Copying a file before it leaves the data center to provide in-house backup.
- Logging out a file when it is removed from the file library or off premises storage (time, date, and method of replacement also should be noted).

Where a backup copy of the newly created master file cannot be quickly removed from the data center, copies of pre-processing transaction files should be removed from the site. This would ensure the ability to recreate a master file with current information.

EQUIPMENT CONTROLS

Equipment controls refer to procedures that prevent or detect unauthorized program execution and computer usage. These controls are usually more effective in detecting when and how unauthorized use occurred rather than in preventing it.

Equipment controls basically consist of the console printer, internal CPU clock, and system activity logs. The console printer indicates communication between the operator and the machine. The internal CPU clock allows the computer to show a time for each job initiated. Console printer paper should be retained intact after each day's processing for management or audit review.

Operator console activity may be stored on disk or tape and exception items extracted for management and audit review. Console logs are a valuable management tool and audit trail which should be used properly by operators.

System activity logs are files created and maintained by the supervisor program. System activity logs record communication between the computer and the operator, and between different parts of the computer system. They cannot be suppressed by the operator if the operating system is properly restricted. The logs are maintained on disk or tape and should be

printed periodically for management and audit review.
Job accounting software or audit retrieval software is used often to summarize a large volume of data. Detailed system usage reports can be developed, and the detail provides an excellent audit trail. A summarized version of such data is appropriate for periodic reports to senior management for all but the smallest installations.

Even the most sophisticated equipment control will lose much of its effectiveness if proper operating procedures are not instituted and maintained. As with nearly all other areas of IS, procedures may range from basic to sophisticated. In all instances, certain minimum procedures should be in effect, including:

- The computer room should not be left unattended while the computer system is in operation. This will help prevent unauthorized use of the equipment as well as save valuable time in the event of a system problem or emergency situation.

- At least two computer operators should be assigned to each shift where practicable. This ensures that one operator will not be able to do any unauthorized work and provides personnel backup.

- Operators must not be allowed to unilaterally override any hardware or operation system checks. This refers to internal label checks, read/write checks, etc., and minimizes the likelihood of processing the wrong data or destroying live data.

- Operators should be required to run all jobs according to the schedule to prevent unauthorized jobs from being run.

- Operators should not allow non-authorized personnel to run the equipment. This applies to all persons who are not console or equipment operators. It will guard against unauthorized use of the computer, especially for systems or applications programmers whose control may be excessive if allowed access to computer operations.

OPERATOR CONTROLS

Computer operators generally have access to programs and data on the system through the equipment and may exercise latitude (equal to the flexibility of the hardware and software environment) in dealing with day-to-day processing. To establish an adequate level of security and internal control, specific rules should be written to limit the scope of and properly direct operator activity.

Rules common to most computer centers are:

- Operators should not execute data or software-altering utility programs without proper authorization. Such programs should be either removed from the system and placed under separate control or maintained under the password protection of an automated library routine (see Chapter 12).

- Operators should not have access to source programs or program listings. Access to other documentation not required for the processing of applications also should be restricted. This will help prevent operators with programming knowledge from making unauthorized changes to production programs.

- Operators should not perform any balancing functions other than run-to-run controls.

- Operators must observe all security procedures including proper library procedures. This will prevent unauthorized access to the equipment, data files and program libraries.

- Operators should initiate the execution of only those programs submitted in accordance with established data center procedures.

LIBRARY CONTROLS

Library controls are procedures to maintain, and prevent unauthorized access to data files, programs, and documentation. There are several libraries in any computer installation. A physical library exists for data and program files, whether they are on magnetic disk or tape. This library should be a secure room area where files can be stored adjacent to the computer room to facilitate the retrieval and storage of processing files. A physical library also exists for system and program documentation, generally in the systems and programming area (see Chapter 12 for additional information). Operator access to systems and programming documentation should be restricted

In addition to physical libraries, several types of program and file libraries are usually part of the computer system. Program libraries consist basically of three types: test, production and private. A test library contains those programs or modules currently being modified or developed by the programming staff. Production libraries contain programs used to process the center's work. Private libraries are sometimes used to retain software that does not conveniently fit the other two categories. The existence and use of private libraries should be addressed in installation standards and be closely monitored by operations management. For each of these program libraries, both a source version and an object version of the library are generally maintained.

Lacking any restrictions, an operator can read, copy, execute, rename, delete or replace a program from the computer system libraries. Since these program library maintenance functions should be restricted, many installations use a library software package for program library control. Some packages are RACF, LIBRARIAN, SECURE, PANVALET, and PANEXEC. Such packages are available through equipment vendors and commercial software firms. In addition, some installations have developed their own library routines. Regardless of the package, library software usually performs a combination of the following functions:

- Restricts access to source (and possibly object) programs on an hierarchical basis, often using a key or password which denotes the authority level of an individual user. For instance, operators might be restricted from access to the test and production library source versions, but allowed access to production library object versions. Restricted library maintenance functions might be reserved for the shift or operations supervisor. When on-line interactive programming is practiced, programmers might be authorized to change test libraries, but not production libraries. Further restrictions could be imposed by application, according to assigned responsibility for programmer maintenance of an application.

- Maintains on a separate file the date and time of access, type of operation performed (such as execute, copy, rename, and read), and identity of the individual (or program) which accessed the module.

- Provides periodic printed reports of the previous information, and:

  - The date last changed or renamed.

  - The version number.

  - The number of times executed or accessed since previous report.

  - The program's status, e.g, test, production, active, inactive.

The control, recording and reporting capabilities of library software vary. Occasionally, such software is adapted to control access to data files in the same manner. In those instances, the proper password often is in the updating object program. When passwords are used, they should be changed periodically and suppressed or made illegible on output.

A second type of software associated with data file libraries is the automated data file inventory. Although a manual inventory of data files can be satisfactory, many installations automate the process of listing the physical location of a file. Although useful, such a system should not be confused with library control software because the function differs substantially.

Some basic considerations for controlling access to files and libraries in all installations are:

- Assigning specific responsibility for the maintenance of production libraries. This will help prevent storing different versions of a program in both the source library and object library. In addition, this function should ensure that source programs supporting each object module are in the library and that all obsolete modules are promptly removed.

- Providing proper authorization to operations personnel to support any changes to production libraries. This requirement is essential for preventing unauthorized changes. The audit trail thus created should be easily traceable to the program change/project request approval mechanism existing in the systems and programming department.

- Denying operators access to magnetic media other than those required for processing application. Although this requirement may not be feasible in smaller operations, it is essential in centers using a significant number of magnetic files. Without it, accurate inventory controls of those files cannot be maintained. In addition, it will minimize the possibility of processing the wrong file or destroying live files.

- Prohibiting operators from executing programs from test libraries during production runs. Permitting this will circumvent most controls included in the procedure for placing programs into a production status. This procedure, known as cataloging, would include such controls as: (1) requiring proper authorization for placing a new version of a program into the production library, (2) verifying that the program has been adequately tested, and (3) requiring that program documentation has been developed or updated.

Controls over access to on-line program files also are discussed in Chapter 12, Systems Development and Programming (Program Security), and in Chapter 14, Security Physical and Data (Program Security).

CONTROL OF DATA FILE MEDIA

Computer-based records (disks, tapes, drums, or cells) are critical to the operation of an institution. Care must be taken on all computing systems when storing various media to ensure adequate protection against physical hazards.

Air-conditioning and humidifying equipment should be used to maintain suitable temperature and humidity levels for stored media. Consideration also must be given to the media’s susceptibility to destruction by electromagnetic field radiation from generators, radar installations or other power sources located nearby. For many computers, especially smaller systems, such as minicomputers, microcomputers and LANs, the files are retained on the computer's fixed disk at all times. The loss of these files without proper backup could cause disruption of business operations and a significant investment of effort to recreate the files from manual records.

Damage or loss of media through fire and other disasters is an important control consideration. Even though a fire may occur in an area adjacent to the media storage room or elsewhere in the building, the resulting heat could destroy data recorded on tapes, disks and similar media. In addition, water used by fire department personnel in combating fire may cause extensive damage to media.

Physical security and control procedures for current and backup data must be as effective as preventive measures installed to protect media against environmental disasters. Ideally, all on-site data files and scratch tapes are stored in a separate room adjacent to the computer equipment. Access to that room should be limited to authorized personnel (normally data file librarians and, in emergencies, shift supervisors). Tapes and disks should remain in this room, i.e., library, unless they are needed for production, are destined for off-site storage, or there is advance management authorization for removal.

If emergency access to the library is required, written procedures should provide that a record is made and reviewed by installation management as soon as possible.

The most desirable location for housing backup is in a separate building away from the data center so that a disaster occurring at one location likely would not affect both sites. However, remote (or offsite) backup should be readily accessible in the event on-premises files become impaired. The same environmental and security considerations must be observed for backup files as for those in the data center library. In addition, sign-in and sign-out records should be maintained, and there should be dual control access procedures at the remote storage location. If management maintains that on-site backup provides adequate protection, the board of directors should review and approve this procedure with its associated risks.

In data centers where only one tape librarian is employed or the position is part-time, controls over access to the tapes and disks are as important as they are in larger data centers. Control may be achieved by locking all data files in a fire resistant vault and by using dual custody procedures to remove files from the vault. If the vault does not have two separate combination locks, the numbers used for the combination can be split between two people. Care must be taken in selecting these persons. The effectiveness of the desired controls could be compromised if both parts of the combination were given to two persons performing the same function. Procedures may be established to allow a shift supervisor emergency access to the tape/disk library in the absence of the librarian. These access procedures should be recorded and reviewed by management.

Tape and disk library procedures should encompass:

- Automated tape library systems or manual procedures in use.
- The daily housekeeping requirements.
- Accountability for newly purchased tapes and disks and retiring old or worn media from active use.
- Periodic inventories of all tapes and disks.
- Retention check and retention schedule for application and program data maintained on tapes or disks.

In all cases, media stored in magnetic form must be protected from loss and unauthorized access. Management should view any compromise of effective control procedures as a possible source of financial loss. Such risk is possible whenever an employee either intentionally or unintentionally – supplies confidential customer information to unauthorized parties. This could result in the financial institution losing business and customer confidence, and being subject to legal action.

A simple but effective method of protecting data on magnetic tape is the file protect ring (read/write ring) which, when inserted in the tape reel, allows information to be recorded. When the ring is removed, information recorded on the tape cannot be overwritten.

This feature may work in reverse on some equipment, but the concept remains the same. Some installations may leave the file protect rings in the tape reels at all times and use an automated tape library management system to determine when a tape may be overwritten.

Disk files can be protected by software controls. One such control is called a file protect feature. This control is a label checking routine that, upon opening a file, compares the creation date, volume number, data set name, and scratch date against the information contained in the program or job control cards. Any discrepancies, such as unexpired scratch date, wrong volume number, or data set name, will be displayed on the console. If an override is intended, the operator must respond through the console. All operator overrides should be logged and be subject to supervisory approval and review.

Some data centers have installed data and program file management systems that help preclude accidental destruction by operator error. However, these systems can be intentionally compromised or bypassed by knowledgeable operators.

The best procedural control is to use external and internal labels. External labels enable operators, tape and disk handlers, and librarians to easily identify the correct tape or disk. In some data centers, color coded tape reels or disk covers are used to distinguish files.

Where descriptive labels are used, any written procedures should be reviewed and compared to actual practices and hard copy records, such as the tape history card. File creation and expiration dates also should be compared to retention schedules. In most data centers using external label identification, the absence of a label indicates that the tape or disk has been released for reuse (scratched).

Many installations using automated librarian systems require only the serial number of the tape or disk to be displayed on the external label. Contents of each tape or disk can be determined by referencing the automated library system reports or by interrogating the library control system via terminals.

Internal labels reduce the possibility that an incorrect tape or disk will be used. However, an operator can often override internal labels. Operators should be informed, in run instructions and verbally, not to override internal labels without prior supervisory approval.

When used, internal labels are located at the beginning and end of data on the file. The header label generally contains the name of the file, the creation date, a volume serial number, a reel sequence number and, in some cases, the date the file expires. The trailer label may contain a record count of the number of records or blocks of information between the header label and the trailer label. It may also provide control totals and information signaling the end of the file or reel. Internal labels should be standardized throughout all applications, subprograms, test files, master files and transaction data files. The use of nonstandard labels may force computer operators to override labels from time to time, diminishing the effectiveness of this control and increasing the possibility of accidental destruction of data and program files. In addition, the efficiency of production jobs may be reduced because nonstandard labels require manual intervention.

Once data and programs are contained in the computer's memory, boundary or storage protection can prevent the data and programs from entering areas of memory designated for other data records and programs.

HOUSEKEEPING

The computer operations personnel must maintain a clean, neat and orderly working environment. Cleanliness in the computer room and surrounding areas decreases the possibility of fire and damage to the computer and peripheral equipment. This is accomplished by:

- Preventing the accumulation of trash in or near the computer room.
- Dumping waste baskets outside the facility to reduce dust discharge.
- Shredding, or otherwise controlling before disposal, waste material containing confidential information.
- Prohibiting eating, drinking, and smoking in the computer room to prevent spills and ashes from damaging equipment.
- Limiting the supply of paper, forms, magnetic media, and other combustible materials located in the machine room(s) to the amount necessary to complete one day's work.
- Maintaining excess forms and supplies in a fire-resistant storage area outside the computer room.
- Permitting only small quantities of cleaning fluids, such as those used to clean tape drives, in the computer room. In general, flammable liquids should be stored away from the computer room and paper storage areas.

EMERGENCY PROCEDURES

Steps to be followed during and immediately after an emergency should be well documented. Since it is not safe to assume that security procedures will prevent the occurrence of an emergency, they must be developed to address such threats as fires, floods, sabotage, riots, bomb threats and acts of nature in proportion to their relative risk of occurrence.

Emergency procedures should personnel and property during emergencies. Instructions for shutting off utilities, powering down computers, protecting data files and documents, activating fire extinguishing systems and other fire fighting equipment, personnel evacuation, and securing valuable assets should be detailed for each area of responsibility, e.g., computer operations, programming, input/output, and end-user processing. The emergency procedures also should provide restart and recovery procedures.

The procedures should be posted conspicuously throughout the organization with implementation responsibility delegated to specific individuals. This reduces the possibility of equipment damage and minimizes the risk for the data center as well as the remaining employees who depend upon computer equipment. Periodic fire and emergency evacuation drills should be conducted and feedback from employees should be encouraged to assess the feasibility of the plan.

TRANSACTION PROCESSING

Financial institutions must receive, record, and process customer transactions in an accurate, reliable, and timely manner. The integrity, reliability, and accuracy of data depends on the establishment of proper control procedures throughout all phases of transaction processing. Whether the control procedures are manual, automated or a combination, coverage should include transaction initiation, data entry, computer processing, and distribution of output reports. These control considerations apply to new technologies such as truncation of items, the electronic presentation of checks, and electronic return items.

The control procedures relating to transaction processing discussed below are neither all inclusive nor recommended for all situations. Each processing environment must be evaluated individually to determine if data integrity is maintained throughout the transaction cycle.

Transaction Controls

The following are important internal, transaction control considerations:

- Duties must be segregated and management supervision should oversee transaction input processing and output functions.
- Overnight control of dollar totals for rejects and holdover items must be well defined and effective.
- Work returned from processing must be reconciled and balanced to the previously established control totals.
- Exception items must be cleared in an expeditious manner (exceptions are contrary to effective control and create potential risk to the financial institution).
- Exception reports must be reviewed by key officers and operation supervisors.
- All output must be produced, properly distributed, and controlled.

Complete control must be maintained over all input documents received at the data center. Input received from one user may need to be separated from that of other users. An effective control over batches of work is recording the batch number and corresponding batch dollar total on a standardized form when the work is initially received at the data center. A separate form should be used for each user.

The department receiving the daily work from users may have a variety of duties, depending on the size of the data center operation. In large installations, the receiving department clerks may spend an entire shift combining batches of work into blocks for capture. In small installations, the receiving clerks may receive the work, log it in, combine batches to make blocks, capture the data through MICR reader/sorters, reconcile the processed work, and collect all entries and reports for return to the users. This is a breach of segregation of duties and should be avoided. Although receiving clerks may accept work for set up and capture and receive entries and reports after reconcilement for return to users, they should not capture or reconcile the work as an additional duty.

Generally, segregation of duties must be achieved so that an individual is not responsible for any two of the following functions:

- Input preparation.
- Operating data input equipment.
- Operating computer and sorting equipment.
- Preparing rejects and nonreads for re-entry.
- Reconciling output.
- Distributing output.

Management must always consider segregation of duties in identifying the desired controls in any size data center operation. Computer operators' duties should be restricted to the operation of the computer, i.e., they should not perform any balancing function. If this is not possible, other duties should be confined only to secondary functions. Segregation of duties becomes increasingly important in an automated environment because critical functions are concentrated in fewer hands.

TRANSACTION INITIATION AND DATA ENTRY

Transaction processing systems convert data from source documents, checks and customer transaction tickets to machine readable form. Three common methods of capturing source document data for information systems are: item capture using magnetic ink character recognition (MICR) equipment, item capture using optical character recognition, and terminal entry.

Item MICR Capture

MICR encoded documents are generally pre-encoded with account number and other transaction information, except for the dollar amounts, to nationwide standards accepted by all financial institutions using data processing equipment. The encoding of dollar amounts is usually performed on proof machines with built-in balancing features during the processing cycle. In some cases, as in the case of installment and mortgage loan coupons, the dollar amount is pre-encoded.

One method of establishing control in item MICR capture is to limit the size of each batch of entries for data processing to no more than 150-300 items. When looking for differences, small batches are easier to handle and reconcile by user personnel and the data center clerks.

Proof Operations

The teller work, and work from other departments is bundled in batches with a batch ticket showing the dollar total of all the items in the batch. At the item processing center or prior to receipt, transactions are processed through a proof operation where the teller work is MICR encoded, proved, and balanced. Batches are consolidated into blocks and block tickets prepared for the total of all batches in the block. The trays of block work are passed to a high speed reader sorter where the MICR information on the checks and transactions tickets is captured by the computer for processing. The transaction tickets and checks are sorted during this activity. At the end of the workday, all the financial and application system item capture report totals are balanced and reconciled to the appropriate applications.

The total dollar amounts of batches submitted for daily processing should always be listed on a transmittal form from departments submitting the work. The transmittal form provides a total of batch debits and credits for each application. This control feature furnishes an audit trail for reconcilement to the general ledger and gives personnel dollar totals to balance the item processing capture runs. User departments and the proof areas should develop control totals since these amounts form the basis for all internal accounting controls i.e., subsequent run-to-run totals and final output records. This principle of internal control is equally applicable to all methods of data entry, whether MICR, key-to-disk or key-to-tape.

In small branches and departments lacking proof equipment, tellers or other branch personnel may prepare batches of checks, deposits, payments, etc., by running adding machine listings of dollar amounts, to develop batch control totals.

In offices and departments with multipocket proof machine equipment, these steps usually are performed:

- A proof machine operator enters the total for each credit and offsetting debit into the machine which encodes the item and sorts credits and debits to selected pockets.

- The dollar amount for each credit and debit entered is accumulated on a separate tape listing for each pocket to which the entries are sorted.

- Periodically the entries are extracted from each pocket and a total is taken for entries run to that pocket.

- Entries are bundled to make a batch with the tape listing from the pocket.

- A batch header is made, indicating the total dollar amount of the batch. Batches are accumulated throughout the day in this manner. At the end of the day, grand totals are taken for each pocket in the machine. These totals represent the control totals for all work processed that day.

Some financial institutions set up regional proof centers to reduce operating costs. These centers operate in a manner similar to the proof department of a single branch, but perform the proof operation for many offices.

In small branches, large branches or unit offices, the teller receiving the entries may prepare the manual batch. However, a second person should check the batches and prepare control totals for all batches on the transmittal form. In branches with proof equipment, tellers should not be permitted to run the proof machine. In financial institutions with multipocket proof machines, operators prepare the batches of work for the day and a supervisor checks the batch totals and control totals prior to the work being shipped for processing.

Proof-of-Deposit

Another method of proof operations used by many institutions is that of single pocket proof-of-deposit (POD). Under this method, all items are pre-encoded except for the dollar amount. The dollar amount is encoded in the proof operation and debit and credit items are sorted into one pocket. As each credit is entered, the amount is locked into a register. The corresponding debits are then entered and the amount of each debit is subtracted from the credit amount. No further credits can be entered until the preceding credit is reduced to zero. This method proves each deposit as well as an overall debit and credit totals.

The POD items are then processed through multipocket reader sorters and sorted by transaction type. Computer dollar totals are accumulated for each pocket for posting to the respective general ledger accounts. Rejected items are generally posted to overnight general ledger suspense or holdover accounts and prepared for resubmission through the proof department. In institutions that charge the appropriate general ledger control account with the proof department totals for the day, totals representing rejected items are reversed the next day. These rejects are again prepared for resubmission and given to the proof department with the next day's work.

In institutions with advanced systems where the general ledger has been automated, the daily entries are accumulated in batches at the individual or central proof departments. The entries are charged to the data center through the head office clearing account, branch clearings account or a computer work-in-process account and forwarded for processing. In these institutions, the data center charges the total of captured and rejected items back to the clearing or work-in-process account. Branch and user department personnel manually prepare entries as required. In other institutions, as processing of each major application is completed, the resulting general ledger entries are generated by the computer, i.e., branch/user personnel do not have to prepare manual entries to update the general ledger. Items for the day that cannot be processed are returned to the originating branch or user department and charged to them through a control account (e.g., unposted debit/credit account).

Unposted transactions should be researched by the user department or office that submitted the items, then reversed from the control account with entries posted to the proper customer or detail account. When the general ledger is automatically posted, the branches or departments should be restricted from making manual entries directly to control accounts without passing the items through the normal process.

Optical Character Recognition

Another means of capturing data similar to MICR capture is by Optical Character Recognition (OCR). The data is either printed or typed on forms using a special type font. An OCR machine then reads the data as input. This method is now being added to some MICR reader/sorters to reduce reject rates and is widely employed in credit card operations. OCR, however, is not in common use in the financial industry.

BATCH PROOF AND BALANCING CONTROL

Upon receipt at the data center, the branch or department work is prepared for processing on high-speed MICR reader/sorter equipment. Each batch of debits and credits should contain a batch header or adding machine tape listing indicating the total dollar amount of the items included in the batch. Usually, a clerk encodes a batch number on a batch header card provided, or creates a batch header and assembles the batches into blocks of items. Each block has a header card that contains the total dollar amount of all batches in the block and a block number.

Blocks are then processed through the reader/sorter equipment and the MICR information captured by the computer. Items rejected from the initial capture run may be run through a second time. The resulting rejects should be maintained separately and sent to the reconcilement clerks with a hard copy listing of captured items. This hard copy listing contains:

- Batch number.
- Block number.
- Item capture number (each item is sequentially numbered on some systems for tracing purposes).
- Account number.
- Dollar amount of each item.
- Batch and block dollar control totals.
- Dollar amount that each individual batch and block are out of balance.

After MICR capture, the work is balanced and reconciled by the user department. A reconcilement form has the total dollar amount of debits and credits submitted for processing and tape listings of the dollar amounts in each batch. These forms and listings assist in reconciling the work submitted for processing to the captured item and the rejected item totals.

The reconcilement clerks balance each batch of debits and credits to the batch capture reports as soon as the report is produced. As each batch is balanced, entries that were not captured on the first or second run are accumulated, and a tape listing is made of the dollar amount of each item. These rejected items are sent to the department that handles reject reentry items. The reject items are then processed with the normal work. Entries that are rejected again are returned to the reconcilement clerks for final balancing, then to the user department for research and correction.

Check Inclearings

Many financial institutions have arranged to exchange local check inclearings (checks drawn on themselves that have been deposited at other financial institutions) to be delivered directly to the data center that services the institution. The inclearings are usually received at the data center during the early morning hours of each work day and posted to depositors' accounts. Settlement between the drawee institution and the deposit financial institution may be made through the Federal Reserve Bank, local clearing houses or a correspondent financial institution.

In such cases, the financial institution upon which the checks are drawn is notified of the total dollar amount of items by advice, and the data center receives the actual items. Inclearings are processed during the day in the same manner as checks processed at night when the day's counter work is received from the financial institution. When the reconcilement clerks complete the reconcilement procedures for the financial institution's counter work, the dollar totals for the inclearings received that morning are combined with the counter work totals. The reconcilement form submitted by the user is completed to show:

- Total dollar amounts received from the financial institution.
- Total dollars received through the inclearings.
- Net captured good items and items drawn on other financial institutions that were missorted.
- Rejected items.
- Holdover items.

The beginning and ending totals of the reconcilement should balance unless any free items (enclosed not listed) were sent and not charged to the data center or items were omitted (listed not enclosed) from the shipment. In these cases, the dollar figure of transactions charged to the data center is incorrect. Therefore, appropriate adjustments should be made on the reconcilement form, and the user area or institution should be notified.

Most data centers attempt to retain the checks captured during the initial run in batch and block sequence until reconcilement clerks have balanced all the work for the day. In some data centers (usually high-volume centers), this is not considered practical and the entries are fine sorted immediately after the primary capture into the financial institution, branch and account number sequence.

Microfilming

Before transporting source documents from branches or departments for item processing, all items should be microfilmed or duplicated. Although most institutions microfilm checks that are sent to other financial institutions, they may not microfilm checks, deposits and internal entries processed to their own accounts when the items are transported to their data center or a service bureau. When shipments of the transaction documents and checks are not recorded on microfilm, the financial institution's senior management should be aware of the risk posed by loss of the shipment while in transit.

TERMINAL ENTRY

Manually entering data into computers via terminals is a common practice. Most widely used are key-to-disk or key-to-tape terminal entry systems. In these systems, data from source documents is entered on magnetic media via key-to-disk or key-to-tape equipment. Data also may be entered directly into the application files from a user department terminal. Electronic input may be received directly from teller terminals, automatic teller machines (ATMs), Point-of-Sale (POS) terminals, client-server terminals, PCs, etc. In terminal entry system, input can be displayed on a video screen as it is entered, edited manually or programmatically, and stored in memory for verification. Key-to-disk and key-to-tape systems are able to produce statistical information to monitor the efficiency of the data entry department. All systems should be able to provide audit trails including source, operator ID, terminal ID, date, and time.

Errors can easily occur when operators convert data from source documents to a machine-readable form. Rejects can be significantly reduced if during manual entry, operators are informed of input errors which can be immediately corrected. Terminal software programs and system software can provide a high degree of error control by using the following techniques:

- Character/field count – A check of character and field count totals for comparison against totals generated as a result of the original data entry. This would indicate the loss or addition of characters or fields to magnetic data file media.

- Truncating fields – An automatic provision which provides right round off or truncation of fields which exceed maximum length.

- Checks for completeness – Programmed checks to ensure that all required entry fields are filled.

- Dollar and item count totals – A necessary tool to prove key entered batches of dollar and non-dollar transactions to preestablished control totals.

- Reasonableness checks – Programmed comparisons of data entered to predetermined absolute values or relative limits of reasonableness.

- Dual-field entry – When the same input appears twice, a check is made to ensure that both fields match.

- Verification check – Input data is echoed back to operator usually on CRT for validation.

- Sequence checks – Programmed checks of key fields in records to ensure proper sequence of data entry.

- Check digits – System performs an algorithmic operation on numeric fields, the result of which should determine the last digit used to ensure valid account numbers.

The software programs providing this type of control should be secured and written, or modified only by programmers with adequate security clearance. Additional controls used before to processing to ensure the integrity of data entered include using hash totals, block and record counts, and cross footing balancing.

Similarly, input editing, other programmed controls and control totals should be employed in on-line file maintenance and memo posting programs.

Batch control totals can be developed for terminal entries by listing and accumulating the dollar amount fields at the user level (some key-disk or tape units do this automatically). Batch totals should be developed for the dollar amounts on entries to achieve effective control. Specially prepared payment cards are used on some applications, principally installment and real estate loans. These cards are produced when the accounts are initiated. The payment coupons are pre-encoded and preprinted with the account number, the dollar amount, type of account and, in some cases, the month payment is due. The payment coupons also can be batched and totals developed for control purposes.

Data entry departments should have documentation containing illustrations of all types of input forms processed with complete step-by-step instructions entering the information on the form. The manual should serve as a training guide for new operators and for day-to-day reference. The key-to-disk and key-to-tape systems can retain and display on the video screen a format of each input form used, showing the data fields that are supplied with input.

In summary, non-MICR documents submitted for data entry that have dollar totals on the entries should be batched and totaled. Control totals for the day's work and a reconcilement form must be given to the data center. After capture, the reconcilement clerks must reconcile the output batch by batch to the item processing capture reports. All other verification of data entry source documents should be performed through a second, independent keying operation or by clerks in the user department. Whenever control totals are developed for data entry work, the work should be charged to and from the data center to ensure accountability.

OUTPUT DISTRIBUTION AND CONTROL

A financial institution's confidential information records must be protected regardless of the media they are recorded on. All printed output and processed source documents must be safeguarded to ensure that the material is forwarded to the appropriate user departments. This section addresses the distribution of output reports in paper form. However, distribution considerations may include Remote Job Entry (RJE) transmissions; network and desktop printers; on-line terminal reports; and CD-ROMs. Whatever method is selected to distribute report information, controls should be established to ensure the proper and timely distribution of the report media.

One method of ensuring proper distribution is to establish a distribution function or department similar to that of a mailroom. Whether output reports and source documents are distributed by messengers, common carrier, or privately contracted courier service, delivery receipts for all data containers should be obtained. Courier containers with transported items should be locked; the data center and user each should have a key.

A distribution control manual should be available which contains:

- A listing by name of all reports produced for applications processed.
- Decollation and bursting instructions as required.
- The number of copies of each report produced for each branch or department.
- Each report's frequency.
- The priority for each branch, department or report in the delivery schedule.
- Special handling instructions.

Separate checklists should be developed to record all daily, weekly, monthly and quarterly reports produced for each application. Procedures should ensure that all required reports are received by the distribution department. A computer program can be written that will generate a list of the day's reports and indicate whether or not the report was produced. Alternatively, the list could reflect only the reports produced or not produced. Such a checklist should be used by both the distribution department and the user department. User areas should review output received for acceptability and consult the report checklist to determine compliance with established distribution policy. Requiring users to sign or initial receipts for computer output may further data control.

The institution's distribution department should review all reports for legible printing, proper alignment of forms and possible errors (such as lines of unsuppressed code or strings of meaningless characters). Also, control totals appearing on related reports should be cross-checked to help ensure their accuracy.

Many data center installations are using computer output microfilm (COM) to replace paper reports. A COM device takes report information from a computer and records it on microfilm. It saves considerable storage space and is far cheaper than paper output. The most common microfilm recording media is microfiche, a card containing multiple images that is displayed on a viewer.

A financial institution's confidential information records must be protected regardless of the media they are recorded on. Controls over the processing, handling and transporting of COM media must be at least as secure as those for other file media. Controls must be established over the number of copies produced and the storage or disposal of all copies. The portability of this type of media (relatively small sheets of film needing only a simple projection device to be read) underscores the importance of strict accountability and access control over this output media.

REVIEW AND RECONCILEMENT OF OUTPUT

The user or an independent control department should reconcile all entries from daily processing to the totals established when the entries were submitted and to the respective general ledger control account. Adjustments must be made for inclearings received at the data center, entries that were missing, extra entries and rejected or nonpostable entries.

In reviewing output, the user area or an independent control department should:

- Double check figures on the transaction reconcilement form originally submitted to the data center.
- Double check the figures prepared by the data

center on the transaction reconcilement form.

- Complete an additional reconcilement form for balancing the trial balance and other report totals to the general ledger control account.

When the general ledger is automated and posting entries are made by the computer, the application totals will tie into the general ledger figures without adjustment. In such cases, it is necessary to investigate the controls over rejected and holdover items and to determine the propriety and age of items in suspense accounts.

Using the demand deposit application as an example, checks captured and posted as good items normally will be reviewed when they are filed. Captured deposits may be filed with checks and returned to the customer or they may be stored by the financial institution for reference. In some institutions, larger dollar amount deposits are compared to the daily posting journal or the check file drawer and the signature card to verify the number and name on the deposit. All other entries, such as rejects, nonreads, and nonpostables, must be reviewed individually.

Inadequate reconcilement procedures by the data center's independent control section or in the user areas may impair the financial institution's ability to return forged, dishonored, or otherwise invalid items within time limits specified by the Uniform Commercial Code, clearing house associations, and various federal rules and regulations. If the return of large negotiable items is delayed, the institution risks significant monetary losses.

All rejected, nonreads, nonpostables, etc., should be segregated from captured items. Each such item should be reviewed by a clerk who either corrects the item for resubmission and posting or returns it to the user area/institution for correction and resubmission, or other disposition. All reject re-entry items should be reviewed by the user department manager. The manager ensures that entries are corrected properly and that the same items are not reappearing as unprocessable. Without such a review, a clerk could conceivably "roll" checks as unprocessable items for extended periods of time.

Exception reports always should be required output regardless of the presence of exception activity or other controls. These reports ensure that both the presence and absence of exceptions are reported. All exception reports, e.g., overdraft, large items, stop/hold, uncollected funds, kiting suspects and past due reports, must be reviewed by financial institution's officers. All reports produced as a result of nonmonetary changes should be compared with the original input, i.e., name and address, new loans, by the responsible user area. Financial institution employees originating or accepting change from a customer should be identified in writing. Also, only under unusual circumstances should master file changes be done without written documentation initiated by the customer.

The responsibility for balancing transaction and trial balance reports to the general ledger often is delegated to a clerk in the user department or to a centralized control division. Periodic unannounced reconcilements should be performed by the institution's auditor or a designated control officer to ensure compliance with established operating procedures. An unannounced reconcilement should include a review of the department settlement sheet, unposted items and exception reports. All large or unusual items should be traced to their final disposition. Records of the reconcilement must be maintained by the auditor or designated control officer, noting the dates of the reconcilement and a listing of all exceptions. Department records should be initiated by the person conducting the check.